REVISION: 1
PUBLICATION DATE: 2022-09-06
DOC. IDENTIFIER: 8DBD000122
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Web Server Buffer Overflow Vulnerability in Hitachi Energy's AFS660/AFS665 series Product

CVE-2020-6994

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a vulnerability report that affects AFS660/AFS665 series versions listed below. Please refer to the Recommended Immediate Actions for information about the mitigation.

An attacker could exploit this vulnerability by crafting a special HTTP request message, to overflow an internal buffer and fully compromise the target device.

Affected Products and Versions

List of affected products and product versions:

Affected products

- AFS660/AFS665

Affected Releases

- Releases 7.0.02 or earlier

Vulnerability ID, Severity and Details

The vulnerability's severity assessment is performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the final vulnerability severity score, is not provided in this advisory as it reflects the potential impact of the vulnerability in the customer organizations' computing environment. Customers are recommended to analyze the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2020-6994 CVSS v3.1 Base Score: 9.8 Critical CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	An improper parsing of URL arguments allows an attacker to possibly exploit this vulnerability, by crafting specially formed HTTP requests to overflow an internal buffer. Successful exploitation may cause a fully compromise of the device.

Recommended Immediate Actions

The Table below shows the affected version and the recommended immediate actions.

Affected Version	Recommended Actions
- AFS660/AFS665 FW 7.0.02 or earlier	Apply mitigation strategy as described in General Mitigation Factors Section or update to latest available release 7.1.05

General Mitigation Factors

Customers are strongly recommended to either use the “IP Access Restriction” feature to restrict HTTP and HTTPS to trusted IP addresses or disable the HTTP and HTTPS server.

In addition, recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Frequently Asked Questions

What is the affected product, AFS660/665?

AFS660/665 are industrial switches from Hitachi Energy, optimized for the data communication of electrical utilities.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could overflow a buffer of the device and fully compromise it.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially formed HTTP requests and sending the message to an affected device. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed. See [1] and [2].

When this security advisory was issued, had Hitachi Energy received any report that this vulnerability was being exploited?

No, Hitachi Energy had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

References

1. BSECV-2020-01 (belden.com)
2. CISA advisory: Hirschmann Automation and Control HiOS and HiSecOS Products - https://www.cisa.gov/uscert/ics/advisories/icsa-20-091-01

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2022-09-06 Same as document publication date	1	Initial public release.

DocuSigned by: